



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0046368
(43) 공개일자 2020년05월07일

(51) 국제특허분류(Int. Cl.)

H04L 9/00 (2006.01)

(52) CPC특허분류

H04L 9/003 (2013.01)

H04L 2209/08 (2013.01)

(21) 출원번호 10-2018-0127420

(22) 출원일자 2018년10월24일

심사청구일자 2018년10월24일

(71) 출원인

동서대학교 산학협력단

부산광역시 사상구 주례로 47(주례동,
동서대학교)

(72) 발명자

이훈재

대구광역시 수성구 청호로85안길 11 선빌라 501호

강영진

부산광역시 사상구 가야대로318번길 84, 205호

김기환

부산광역시 북구 화명대로 87 현대아파트 101동
1501호

(74) 대리인

김석계

전체 청구항 수 : 총 3 항

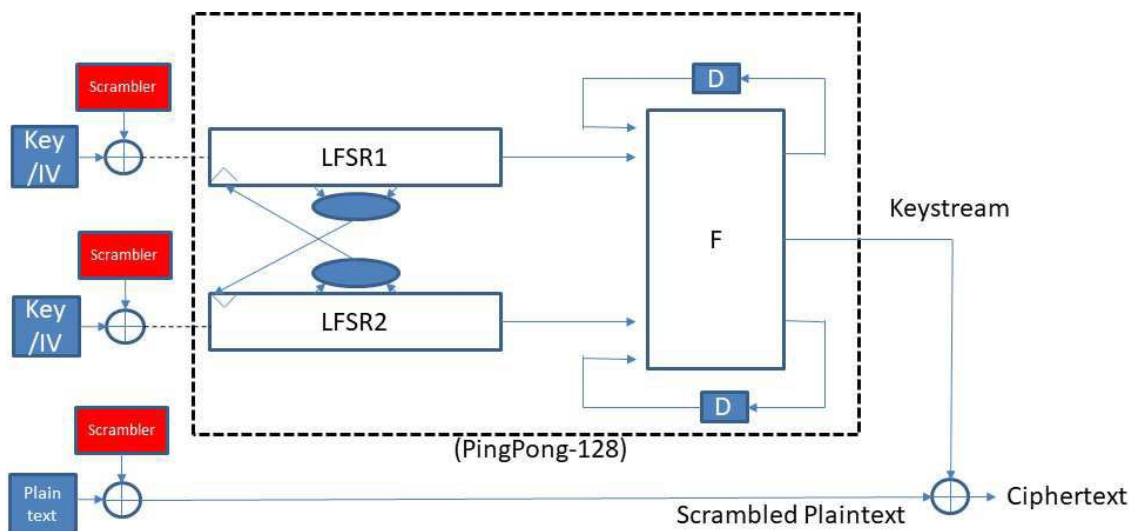
(54) 발명의 명칭 알고리즘의 방어기술 적용방법

(57) 요약

본 발명 알고리즘의 방어기술 적용방법은 두 개의 통신장치 간에 데이터 통신을 할 시, 전력분석공격에 취약한 알고리즘에 전력분석공격에 대한 방어기술을 적용하여 전력분석공격에 대한 안전성 제공하는 것으로,

본 발명 알고리즘의 방어기술 적용방법은 두 개의 통신장치 간에 데이터 통신을 할 시, 전력분석공격에 취약한 알고리즘(즉, PingPong-128 알고리즘)에 전력분석공격에 대한 방어기술을 적용하여 전력분석공격에 대한 안전성 제공하는 현저한 효과가 있다.

대표도 - 도2



이 발명을 지원한 국가연구개발사업

과제고유번호 2018-E-G023-010100
 부처명 교육부
 연구관리전문기관 한국연구재단
 연구사업명 사회맞춤형 산학협력 선도대학(LINC+) 육성사업
 연구과제명 사회맞춤형 산학협력 선도대학(LINC+) 육성사업(산학협력 고도화형)
 기 여 율 1/3
 주관기관 동서대학교 산학협력단
 연구기간 2017.04.01 ~ 2022.02.28

이 발명을 지원한 국가연구개발사업

과제고유번호 2016R1D1A1B01011908
 부처명 교육부
 연구관리전문기관 한국연구재단
 연구사업명 이공분야기초연구사업(기본연구지원사업)
 연구과제명 사물인터넷/무인비행기(IoT/Drone)에 적합한 초경량-고속 암호/인증 및 물리적 해킹 방어

기술 개발

기 여 율 1/3
 주관기관 동서대학교산학협력단
 연구기간 2016.06.01 ~ 2023.05.31

이 발명을 지원한 국가연구개발사업

과제고유번호 1711074107
 부처명 과학기술정보통신부
 연구관리전문기관 정보통신기술진흥센터
 연구사업명 정보통신 방송연구개발사업(정보보호핵심원천기술개발사업)
 연구과제명 무인이동체를 위한 HD급 영상 데이터 및 제어 신호 암호화 처리용 고신뢰 듀얼코어 SoC

및 운용시스템 개발

기 여 율 1/3
 주관기관 (주)네오와인
 연구기간 2018.04.01 ~ 2019.12.31

명세서

청구범위

청구항 1

두 개의 통신장치 간에 데이터 통신을 할 시, 전력분석공격에 취약한 알고리즘에 전력분석공격에 대한 방어기술을 적용하여 전력분석공격에 대한 안전성 제공하는 것을 특징으로 하는 알고리즘의 방어기술 적용방법

청구항 2

제 1항에 있어서, 상기 전력분석공격에 취약한 알고리즘에 적용할 수 있는 방어기술로써, 스램블러와 디스크램블러를 활용하여 랜덤화 방법을 적용함에 따라, 회로가 단순하면서도 차등 전력 분석(DPA)에 대한 방어가 되는 것을 특징으로 하는 알고리즘의 방어기술 적용방법

청구항 3

제 2항에 있어서, 상기 랜덤화 방법은 키 랜덤화 방법과, 평문 랜덤화 방법으로 구분되는 것을 특징으로 하는 알고리즘의 방어기술 적용방법

발명의 설명

기술 분야

[0001]

본 발명은 알고리즘의 방어기술 적용방법에 관한 것으로, 보다 상세하게는 두 개의 통신장치 간에 데이터 통신을 할 시, 전력분석공격에 취약한 알고리즘(즉 PingPong-128 알고리즘)에 전력분석공격에 대한 방어기술을 적용하여 전력분석공격에 대한 안전성 제공하는 알고리즘의 방어기술 적용방법에 관한 것이다.

배경 기술

[0003]

종래의 알고리즘 중에서도 PingPong-128 알고리즘은 전력분석공격에 취약함을 보이고 있다. 상기 PingPong-128 알고리즘에 대한 전력분석공격은 인위적으로 동기여러를 발생시켜 초기벡터로 재동기 시키는 방법을 적용하여 공격하는 것이되, 상기 초기벡터인 iv 는 알려진 값이고, 비밀키인 k 는 알려지지 않은 값이므로, 비밀키인 k 가 알려지게 되어 $(iv \oplus k)$ 의 연산이 실행되는 시점에서 공격하는 것이다.

[0004]

종래기술로서 등록특허공보 등록번호 제10-1202245호의 이체정보로 생성되는 OTP를 활용한 계좌이체시스템 및 방법에는, 온라인뱅킹 상에서 OTP를 활용한 계좌이체시스템에 있어서, 은행에서 사용자가 직접 배부받으며 OTP를 생성하는 OTP생성모듈을 포함하는 모바일 단말기;와 은행서버접속모듈을 포함하는 PC;와 유효한 사용자 인증정보 입력시 기준OTP의 제1암호부와 제2암호부를 생성하는 기준OTP생성모듈, 기준OTP와 이체정보를 전달받아 기준OTP 제1암호부의 특정코드와 기준OTP의 제2암호부의 입력요청을 상기 은행서버접속모듈로 전송하는 OTP 입력요청모듈, OTP와 기준OTP를 비교하여 일치여부를 확인하는 OTP비교모듈, 이체정보에 따라 이체를 실시하는 이체모듈, 사용자별 유일한 값을 가지는 제1개인키, 제2개인키를 사용자 별로 구분하여 저장하는 개인키DB, 사용자별 유일한 값을 가지는 PIN을 사용자 별로 구분하여 저장하는 PIN DB를 포함하는 은행서버;를 포함하되, 상기 모바일 단말기, PC, 은행서버는 네트워크로 연결되어 있으며, 상기 OTP생성모듈은 사용자로부터 PIN을 입력받으면 실행되고, 사용자로부터 이체정보, 상기 모바일 단말기에 저장된 사용자의 제1개인키를 변수로 입력받아 OTP의 제1암호부를 생성하고, 상기 이체정보를 사용자로부터 모바일 단말기로 입력받은 때의 시간정보, 상기 모바일 단말기에 저장된 사용자의 제2개인키를 변수로 입력받아 상기 OTP의 제2암호부를 생성하며, 상기 은행서버 접속모듈은 사용자로부터 사용자의 인증정보와 상기 이체정보를 입력받아 상기 기준OTP생성모듈로 전송하며, 상기 개인키DB는 사용자별 유일한 값을 가지는 상기 제1개인키, 제2개인키를 사용자 별로 구분하여 저장하고, 상기 PIN DB는 사용자별 유일한 값을 가지는 PIN을 사용자 별로 구분하여 저장하고, 상기 기준OTP생성모듈은 상기 은행서버접속모듈로부터 전달받은 사용자의 인증정보가 유효한 경우, 상기 은행서버접속모듈로부터 전달받은 이체정보, 상기 개인키DB에서 검색한 상기 사용자의 제1개인키를 변수로 입력받아 기준OTP의 제1암호부를 생성하

고 상기 이체정보를 사용자로부터 PC로 전송받은 때의 시간정보, 상기 개인키DB에서 검색한 상기 사용자의 제2 개인키를 변수로 입력받아 상기 기준OTP의 제2암호부를 생성하며, 상기 OTP입력요청모듈은 상기 기준OTP생성모듈로부터 상기 기준OTP의 제1암호부와 제2암호부, 상기 이체정보를 전달받아, 상기 이체정보와 상기 PIN DB에서 검색한 사용자의 PIN을 이용하여 상기 기준OTP의 제1암호부의 특정코드를 선택한 뒤, 상기 특정코드와 기준OTP의 제2암호부의 입력요청을 상기 은행서버접속모듈로 전송하고, 상기 은행서버접속모듈은 상기 은행서버로부터 상기 기준OTP의 제1암호부의 특정코드와 기준OTP의 제2암호부의 입력요청을 받으면 상기 사용자로부터 상기 OTP생성모듈에서 생성된 제1암호부의 특정코드와 제2암호부를 입력받아 상기 은행서버로 전송하고, 상기 OTP비교모듈은 상기 은행서버접속모듈로부터 상기 제1암호부의 특정코드와 제2암호부를 전달받아 상기 제1암호부의 특정코드와 상기 기준OTP의 제1암호부의 특정코드와의 일치 여부를 확인하고, 상기 제2암호부와 기준OTP의 제2암호부와 일치 여부를 확인하여 둘 다 일치하는 경우 상기 은행서버의 이체모듈로 상기 이체정보 및 이체명령을 전달하고, 상기 이체모듈은 상기 이체정보에 따라 이체를 실시하되, 상기 제1암호부와 기준OTP의 제1암호부는 입력받은 상기 이체정보, 제1개인키가 일치하는 경우 동일한 값으로 생성되며, 상기 제2암호부와 기준OTP의 제2암호부는 입력받은 상기 시간정보, 제2개인키가 일치하는 경우 동일한 값으로 생성되는 것을 특징으로 하되, 상기 제2암호부 생성시 입력된 시간정보와 상기 기준OTP의 제2암호부 생성시 입력된 시간정보가 상기 OTP생성모듈, 기준OTP생성모듈에 설정된 허용범위 이내의 차이를 가지는 경우 동일한 시간정보로 인식하는 것을 특징으로 하는 이체정보로 생성되는 OTP를 활용한 계좌이체시스템이라고 기재되어 있다.

[0005] 다른 종래기술로서 등록특허공보 등록번호 제10-0713476호의 이동 네트워크에서 고속 핸드오프를 위한 시스템 및 방법에는, 이동 노드가 존재하고, 상기 이동 노드는 제1 액세스 라우터에 의해 관리되며, 상기 제1 액세스 라우터와는 서브넷이 상이한 제2 액세스 라우터가 존재하는 이동 네트워크에서, 상기 이동 노드가 상기 제1 액세스 라우터에서 상기 제2 액세스 라우터로 고속 핸드오프를 수행하는 방법에 있어서, 상기 이동 노드가 상기 제1 액세스 라우터를 통해 상기 제2 액세스 라우터로부터의 라우팅 광고(RA: Routing Advertisement) 메시지를 수신하는 과정과, 상기 이동 노드가 상기 라우팅 광고 메시지를 이용하여 상기 제2 액세스 라우터에서 사용할 아이피(IP) 주소를 생성하는 과정과, 상기 이동 노드가 상기 제1 액세스 라우터에서 상기 제2 액세스 라우터로의 이동을 완료하면, 상기 생성한 IP 주소를 사용하기 위한 트리거(trigger)를 수행하는 과정과, 상기 IP 주소를 이용하여 대응 노드와 데이터를 송수신하는 과정을 포함하는 고속 핸드오프 수행방법이라고 기재되어 있다.

[0006] 그러나 상기와 같은 종래의 구성은 전력분석공격에 취약한 알고리즘(즉, PingPong-128 알고리즘) 사용시 전력분석공격에 대해 방어기술을 적용하지 못하여 안전성을 제공하지 못하는 단점이 있었다.

발명의 내용

해결하려는 과제

[0008] 따라서 본 발명 알고리즘의 방어기술 적용방법을 통하여, 두 개의 통신장치 간에 데이터 통신을 할 시, 전력분석공격에 취약한 알고리즘(즉, PingPong-128 알고리즘)에 전력분석공격에 대한 방어기술을 적용하여 전력분석공격에 대한 안전성 제공하는 알고리즘의 방어기술 적용방법을 제공하고자 하는 것이다.

과제의 해결 수단

[0010] 본 발명 알고리즘의 방어기술 적용방법은 두 개의 통신장치 간에 데이터 통신을 할 시, 전력분석공격에 취약한 알고리즘에 전력분석공격에 대한 방어기술을 적용하여 전력분석공격에 대한 안전성 제공하는 것을 특징으로 한다.

발명의 효과

[0012] 본 발명 알고리즘의 방어기술 적용방법은 두 개의 통신장치 간에 데이터 통신을 할 시, 전력분석공격에 취약한 알고리즘(즉, PingPong-128 알고리즘)에 전력분석공격에 대한 방어기술을 적용하여 전력분석공격에 대한 안전성 제공하는 현저한 효과가 있다.

도면의 간단한 설명

- [0014] 도 1은 본 발명 알고리즘의 방어기술 적용방법의 스크램블 작동 개념도
 도 2는 본 발명 알고리즘의 방어기술 적용방법의 개념도

발명을 실시하기 위한 구체적인 내용

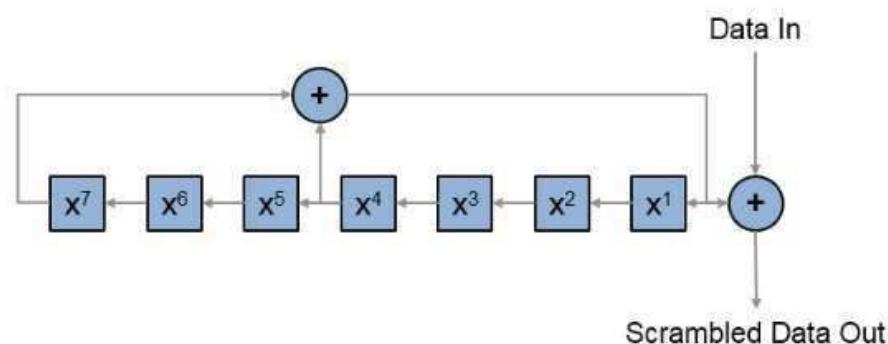
- [0015] 본 발명 알고리즘의 방어기술 적용방법은 두 개의 통신장치 간에 데이터 통신을 할 시, 전력분석공격에 취약한 알고리즘에 전력분석공격에 대한 방어기술을 적용하여 전력분석공격에 대한 안전성 제공하는 것을 특징으로 한다.
- [0016] 또한, 상기 전력분석공격에 취약한 알고리즘에 적용할 수 있는 방어기술로써, 스크램블러와 디스크램블러를 활용하여 랜덤화 방법을 적용함에 따라, 회로가 단순하면서도 차등 전력 분석(DPA)에 대한 방어가 되는 것을 특징으로 한다.
- [0017] 또한, 상기 랜덤화 방법은 키 랜덤화 방법과, 평문 랜덤화 방법으로 구분되는 것을 특징으로 한다.
- [0018] 또한, 상기 두 개의 통신장치 간에 데이터 통신시, 송신측 통신장치에서는 데이터의 랜덤화를 위하여 스크램블러(scrambler)를 사용하는 것이며, 수신측 통신장치에서는 디스크램블러(de-scrambler)로 역변환시킨다음 데이터를 모뎀으로 입력시키게 되는 것을 특징으로 한다.
- [0020] 본 발명을 첨부 도면에 의해 상세히 설명하면 다음과 같다.
- [0021] 도 1은 본 발명 알고리즘의 방어기술 적용방법의 스크램블 작동 개념도, 도 2는 본 발명 알고리즘의 방어기술 적용방법의 개념도이다.
- [0022] 본 발명에 대해 구체적으로 기술하면, 본 발명 알고리즘의 방어기술 적용방법은 두 개의 통신장치 간에 데이터 통신을 할 시, 전력분석공격에 취약한 알고리즘에 전력분석공격에 대한 방어기술을 적용하여 전력분석공격에 대한 안전성 제공하는 것이다.
- [0023] 이때, 상기 전력분석공격에 취약한 알고리즘은 PingPong-128 알고리즘인 것이다.
- [0024] 상기 전력분석공격에 취약한 알고리즘에만 방어기술을 적용하는 것으로, 송·수신 암호에는 방어기술을 적용하지 않아 암호 알고리즘의 성능이 저하되지 않으며, 전력분석공격에 대한 안전성을 제공하는 것이다.
- [0025] 상기 전력분석공격에 취약한 알고리즘의 암호는 두 개의 LFSR과 출력함수 F 및 클럭조정함수들로 구성되어 있는 것이다.
- [0027] 일반적으로 전력분석공격은 CPU, 암호화 회로 등의 하드웨어의 전력 소비 변화를 관찰하면서 정보를 얻는 방식으로, 단순 전력 분석(SPA)과 차등 전력 분석(DPA)으로 나누어진다.
- [0028] 특히, 상기 전력분석공격에 취약한 알고리즘에 대한 전력분석공격은 인위적으로 동기에러를 발생시켜 초기벡터로 재동기 시키는 방법을 적용하여 공격하는 것이되, 상기 초기벡터인 iv 는 알려진 값이고, 비밀키인 k 는 알려지지 않은 값이므로, 비밀키인 k 가 알려지게 되어 $(iv \oplus k)$ 의 연산이 실행되는 시점에서 공격하는 것이다.
- [0030] 상기 두 개의 통신장치 간에 데이터 통신시, 동기 에러는 전체 메시지 또는 남은 메시지의 재전송을 요구하며, 동기식 스트림 암호의 경우에는 안전성을 위해 다른 키 수열이 사용되어야 하는 것으로, 상기 다른 키 수열을 사용하기 위한 키 갱신(rekeying)은, 비밀키(Secret Key)와, 평문상태로 전송될 초기벡터(iv , initialization vector)를 재동기 시키는 방법이 적용되는 것이다.
- [0032] 상기 두 개의 통신장치 간에 데이터 통신시, 송출되는 데이터에서 "0"이 연속으로 발생에 의해 수신단에서 클럭 동기 복구가 어려워지는 것을 방지하기 위해, 송신측 통신장치에서는 데이터의 랜덤화를 위하여 스크램블러(scrambler)를 사용하는 것이며, 수신측 통신장치에서는 디스크램블러(de-scrambler)로 역변환시킨다음 데이터

를 모델로 입력시키게 되는 것이다.

- [0034] 상기 전력분석공격에 대한 방어기술을 적용하기 위해, 하드웨어 게이트 설계단계에서 방어기술을 삽입하는 것이나, 또는 암호 모듈(cryptographic module)의 구성 방법에 따라 방어기술을 추가하는 것으로, 예를 들면, 상기 암호 모듈(cryptographic module)이, FPGA(Field Programmable Gate Array)가 포함된 하드웨어 기반의 고속화 암호 모듈인 경우, 게이트어레이 논리로 방어기술을 적용하는 것이며, 상기 암호 모듈(cryptographic module)이, 마이크로프로세서 모듈을 통한 펌웨어 암호모듈인 경우, 소프트웨어 코딩으로 방어기술을 적용하는 것이다.
- [0036] 상기 전력분석공격에 취약한 알고리즘에 적용할 수 있는 방어기술로써, 스크램블러와 디스크램블러를 활용하여 랜덤화 방법을 적용함에 따라, 회로가 단순하면서도 차등 전력 분석(DPA)에 대한 방어가 되는 것이다.
- [0037] 상기 랜덤화 방법은 키 랜덤화 방법과, 평문 랜덤화 방법으로 구분된다.
- [0038] 상기 키 랜덤화 방법은 키 값과, 평문상태로 전송될 초기벡터(iv) 값에 스크램블러를 적용하는 방법인 것으로, 전력분석공격에 취약한 알고리즘(즉, PingPong-128 알고리즘)에 사용되는 키 길이는 128비트(bit)이며, 키 값이 1비트(bit) 단위로 입력될 때마다 스크램블러로 값을 변화하여 도 2에 도시된바와 같이, LFSR1과 LFSR2에 입력하게 되는 것이다.
- [0039] 상기 평문 랜덤화 방법은 평문 값에 스크램블러를 적용하는 방법인 것으로, 전력분석공격에 취약한 알고리즘(즉, PingPong-128 알고리즘)에 사용되는 평문의 길이는 무제한적이며, 평문 값이 1비트 단위로 입력될 때마다 스크램블러로 값을 변화하여 키스트림(keystream)과 배타적 논리합(XOR, exclusive or)시키게 된다. 수신에서도 동일한 방법으로 적용한다.
- [0040] 본 발명에서는 상기 전력분석공격을 하기 위해 인위적으로 재동기를 시켜도, 스크램블러에 의해 다시 랜덤화 방법이 적용되기에 전력분석공격에 대한 방어기술이 적용되는 것이다.
- [0042] 따라서, 본 발명 알고리즘의 방어기술 적용방법은 두 개의 통신장치 간에 데이터 통신을 할 시, 전력분석공격에 취약한 알고리즘(즉, PingPong-128 알고리즘)에 전력분석공격에 대한 방어기술을 적용하여 전력분석공격에 대한 안전성 제공하는 현저한 효과가 있다.

도면

도면1



도면2

